AMENDMENTS TO THE CLAIMS

1. (currently amended) A system of distributed group management for indirectly authenticating membership of a user in a group in order to manage security for a client on the user side and a server for executing a remote processing request from the user side under a predetermined authorization assigned for every group, provided with

a group certificate issuing apparatus for issuing a group certificate on the client side based on original group information including the name of the group to which the related user belongs when there is said remote processing request and

a group certificate verification unit for verifying a legitimacy of said group certificate transmitted from the client side in said server, wherein

said group certificate issuing apparatus adds an issuance side processed value obtained by ~~processing~~ encrypting the information of the original group information by a cryptographic function to the original group information and defines this as the group certificate and

said group certificate verification unit processes part of the information included in the received group certificate by an identical cryptographic function to obtain a verification side processed value and performs said authentication by confirming that said issuance side processed value and said verification side processed value coincide.

2. (original) A system of distributed group management as set forth in claim 1, wherein

said group certificate issuing apparatus includes secret information assigned to said groups in said original group information and performs the processing by said cryptographic function,

said group certificate verification unit includes said secret information assigned to the

groups in part of information included in said received group certificate and performs the processing by said cryptographic function, and

said group certificate issuing apparatus and said server share identical secret information for identical groups.

3. (original) A system of distributed group management as set forth in claim 1, wherein said cryptographic function is a hash function.

4. (original) A method of distributed group management for indirectly authenticating the membership of a user in a group in order to manage the security for a client on the user side and a server for executing the remote processing request from the user side under the predetermined authorization assigned for every group, comprised of

a first step for processing the information of the original group information including the name of group to which the related user U belongs by the cryptographic function when there is said remote processing request on the client side and issuing a group certificate obtained by adding the obtained issuance side processed value to the original group information,

a second step of processing the information of the received group certificate by an identical cryptographic function to obtain the verification side processed value on the server side, and

a third step of comparing said verification side processed value and received issuance side processed value on the server side and confirming that they coincide, thereby to perform said authentication, and verify the legitimacy of said group certificate transmitted from the client side in said server.

5. (currently amended) A group certificate issuing apparatus comprising part of a system of distributed group management for indirectly authenticating membership of a user to a

group in order to manage the security with respect to the client on the user side and the server for executing the remote processing request from the user side under predetermined authorization assigned for every group, provided with

an issuance side processor for issuing the original group information including the name of group with the related user membership thereto when there is said remote processing request and, at the same time, adding the issuance side processed value obtained by ~~processing~~ encrypting the information of the original group information by the cryptographic function to the original group information to obtain the group certificate.

6. (original) A group certificate verification unit comprising a system of distributed group management for indirectly authenticating the membership of a user to a group in order to manage the security of the client on the user side and the server for executing the remote processing request from the user side under the predetermined authorization assigned for every group, including

a verification side processor for processing information included in the group certificate received from the client side by the cryptographic function to generate the verification side processed value on the server side and performing said authentication by confirming that the issuance side processed value included in the received group certificate and said verification side processed value coincide.

7. (original) A group certificate issuing apparatus as set forth in claim 5, wherein said cryptographic function is a hash function, and said issuance side processor is provided with a hash facility for performing the processing of the hash function.

8. (original) A group certificate issuing apparatus as set forth in claim 7, wherein said issuance side processor centrally applies the processing of said hash function with respect to at

least the group name and the secret information unique to that group, regards said issuance side processed value as the temporary password "temp", and generates said group certificate from at least said group name and said temporary password.

9. (original) A group certificate issuing apparatus as set forth in claim 8, wherein it cooperates with a hash function unit provided in said client, and the hash function unit applies the processing of said hash function m times with respect to said temporary password, regards the obtained issuance side processed value as a one-time password, and a log-in request comprised of at least said group name and said one time password is generated by the client in place of said group certificate.

10. (original) A group certificate issuing apparatus as set forth in claim 8, wherein it cooperates with a unique ID generation means provided in said client, and the unique ID generation means generates an authentication ID for mutual authentication between said client and said server, contains the authentication ID in said group certificate, and transmits the same to said server.

11. (original) A group certificate issuing apparatus as set forth in claim 10, wherein said transmitted group certificate including said authentication ID is received at said server, a server reply obtained by applying a predetermined processing with respect to this is returned to said client, a server reply expected in the client by using the same processing as the predetermined processing and the returned server reply are compared, and when the two coincide, the client authenticates the server.

12. (original) A group certificate issuing apparatus as set forth in claim 8, wherein it cooperates with an encryption processing unit provided in said client, and the encryption processing unit establishes an encryption session from the client to said server with said

temporary password as an encryption key.

13. (original) A group certificate issuing apparatus as set forth in claim 8, wherein provision is made of a log file for recording the log of the session according to each said remote processing request for each of said users, and supervision of each user is performed based on the log.

14. (original) A group certificate issuing apparatus as set forth in claim 13, wherein said temporary password for every said session is included in said log and thereby to identify the sessions.

15. (original) A group certificate issuing apparatus as set forth in claim 8, wherein a unique ID generation means is further included and, at the same time,

said issuance side processor further adds valid term information to said group name and the secret information unique to the group and applies the processing of said hash function, regards obtained said issuance side processed value as the temporary password, and generates said group certificate from said group name, said valid term information, and said temporary password, and

said unique ID generation means generates the certificate ID for identifying these group certificates for every user and adds the same to corresponding each group certificate when the group certificates having the identical contents are issued with respect to plurality of different said users.

16. (original) A group certificate issuing apparatus as set forth in claim 9, wherein a unique ID generation means is further included and, at the same time,

said issuance side processor further adds the valid term information to said group name and the secret information unique to the group and applies the processing of said

hash function, obtains said one time password based on an obtained temporary password and generates said log-in request, and

said unique ID generation means generates the certificate ID for identifying the log-in requests for every user when the log-in requests having the identical contents are issued with respect to plurality of different said users and adds the same to each corresponding log-in request.

17. (original) A group certificate issuing apparatus as set forth in claim 7, wherein provision is made of a user-group mapping storage means, and in the user-group mapping storage means, a plurality of different groups can be assigned for one said user.

18. (original) A group certificate verification unit as set forth in claim 6, wherein said cryptographic function is a hash function and said verification side processor is provided with the hash facility for performing the processing of the hash function.

19. (original) A group certificate verification unit as set forth in claim 18, wherein said verification side processor centrally applies the processing of said hash function with respect to at least the group name and the secret information unique to that group included in said group certificate received from the client side so as to reproduce said verification side processed value as the reproduced temporary password.

20. (original) A group certificate verification unit as set forth in claim 19, wherein said verification side processor is a hash function unit, and the hash function unit applies the processing of said hash function to said temporary password m number of times to reproduce said verification side processed value as a one-time password and confirms that the reproduced one-time password and the one time password extracted from the log-in request including the one-time password similarly generated on the client side coincide to perform said authentication.

21. (original) A group certificate verification unit as set forth in claim 19, wherein, for the mutual authentication between said client and said server, the authentication ID transmitted included in said group certificate is received from said client, predetermined processing is applied with respect to this to generate a server reply, the server reply is returned to said client and compared with the server reply expected in the client by using the same processing as the predetermined processing, and when the two coincide, the client authenticates the server.

22. (original) A group certificate verification unit as set forth in claim 19, wherein it cooperates with an encryption processing unit provided in said server, said encryption processing unit establishing an encryption session from the server to said client with said temporary password as an encryption key.

23. (original) A group certificate verification unit as set forth in claim 18, wherein it cooperates with a log file provided in said server, the log file recording a log of the session according to each said remote processing request for each of said users, each user being supervised based on the log.

24. (original) A group certificate verification unit as set forth in claim 23, wherein said temporary password for every said session is included in said log to identify the sessions.

25. (original) A group certificate verification unit as set forth in claim 19, wherein it receives group certificates added with certificate IDs for identifying these group certificates for every user from said client and allots said plurality of different users to the identical groups by the certificate IDs when group certificates having identical contents are issued with respect to a plurality of different users.

26. (original) A group certificate verification unit as set forth in claim 20, wherein it receives log-in requests added with log-in request IDs for identifying these log-in requests for

every user from said client and allots said plurality of different users to identical groups by the log-in request ID when said log-in requests having the identical contents are issued with respect to plurality of different said users.

27. **(original)** A group certificate verification unit as set forth in claim 18, wherein it cooperates with a group certificate temporary storing unit provided in said server, and, when the assignment of a plurality of different groups is enabled for one said user, it verifies said group certificates received from said client, stores them in the group certificate temporary storing unit, and switches and uses the stored group certificates in accordance with said predetermined authorization necessary for the request with respect to the following remote processing requests.

28. **(original)** A group certificate verification unit as set forth in claim 19, wherein it cooperates with a log-in request temporary storing unit provided in said server, and, when the assignment of the plurality of different groups is enabled for one said user, it verifies said log-in requests received from said client, stores them in the log-in request temporary storing unit, and switches and uses the stored log-in requests in accordance with said predetermined authorization necessary for the request with respect to following remote processing requests.